# PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT REC'D 31 MAR 2005
WIPO PCT

## WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

| | |
|---|---|
| Date of mailing *(day/month/year)* see form PCT/ISA/210 (second sheet) | |
| Applicant's or agent's file reference<br>see form PCT/ISA/220 | **FOR FURTHER ACTION**<br>See paragraph 2 below |
| International application No.<br>PCT/IB2004/052793 | International filing date *(day/month/year)*<br>13.12.2004 |
| Priority date *(day/month/year)*<br>24.12.2003 | |
| International Patent Classification (IPC) or both national classification and IPC<br>G06F1/00, H04L9/32 | |
| Applicant<br>KONINKLIJKE PHILIPS ELECTRONICS N.V. | |

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

| | |
|---|---|
| Name and mailing address of the ISA:<br>European Patent Office<br>D-80298 Munich<br>Tel. +49 89 2399 - 0 Tx: 523656 epmu d<br>Fax: +49 89 2399 - 4465 | Authorized Officer<br>Telephone No. +49 89 2399- |

Form (PCT/ISA/237) (Cover Sheet) (January 2004)

**WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/IB2004/052793

**Box No. I Basis of the opinion**

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

**Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

| | | | |
|---|---|---|---|
| Novelty (N) | Yes: | Claims | 1,14,15,16,17,18 |
| | No: | Claims | |
| Inventive step (IS) | Yes: | Claims | |
| | No: | Claims | 1,14,15,16,17,18 |
| Industrial applicability (IA) | Yes: | Claims | 1,14,15,16,17,18 |
| | No: | Claims | |

2. Citations and explanations

**see separate sheet**

**Re Item V.**

1 Reference is made to the following documents:

D1 : SAITO T ET AL: "Privacy enhanced access control by SPKI" PARALLEL AND DISTRIBUTED SYSEMS: WORKSHOPS, SEVENTH INTERNATIONAL CONFERENCE ON, 2000 IWATE, JAPAN 4-7 JULY 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 4 July 2000 (2000-07-04), pages 301-306, XP010523887 ISBN: 0-7695-0571-6

D2 : MENEZES A J ED - MENEZES ET AL: "Handbook of Applied Cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 408-409,508,55, XP002186996 ISBN: 0-8493-8523-7

D3: BUSSARD L ET AL: "Untraceable secret credentials: trust establishment with privacy" PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 2004. PROCEEDINGS OF THE SECOND IEEE ANNUAL CONFERENCE ON, PISCATAWAY, NJ, USA,IEEE, 14 March 2004 (2004-03-14), pages 122-126, XP010689740 ISBN: 0-7695-2106-1

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject matter of claim 1 does not involve an inventive step in the sense of Article 33(3)PCT.

2.1 Document D1, which is considered to represent the most relevant state of the art to the subject matter of claim 1, discloses (the references in parentheses applying to this document):

a) A method for preserving privacy for a user while enabling the user controlled access to data (Abstract).
b) The user being represented by a user device and identified by a user identity (Fig. 2, Pag. 301 Col. right l. 15-19).
c) The method using at least one certificate that associates data access rights with the user identity (Pag. 301 Col. right l.25-31).

d) Wherein the certificate conceals the user identity (Pag. 301 Col. right l.32-36).
e) A certificate verification process between the user device and a verifier device, a certificate issuing process between the user device and an issuing device, a certificate re-issuing process between the user device and the issuing device (Pag. 302 Col. left l.1-8).
f) Wherein the certificate verification process comprises the steps of the user device obtaining the concealed secret S' corresponding to the certificate (Pag. 305 Col. right l. 30), the user device retrieving the secret S from the concealed secret S' (Pag. 304 Col. right l.19-30), the verifier device obtaining the solution information P from the certificate (Pag. 305 Col. left l.3-6).
g) Wherein the certificate issuing process comprises the steps of the issuing device issuing a certificate (Pag. 304 col. left l.19-30).
h) The certificate re-issuing process (Pag. 305 col. left l.19-30).

2.2 The subject-matter of independent claim 1 differs from the disclosure of D1 in that the authentication process does not use a zero knowledge authentication method but one based on ID certificates.

2.3 The problem to be solved by the present invention may therefore be regarded as how to assure privacy of users.

2.4 The solution proposed by claim 1 does not involve an inventive activity, the reasons being as follows:
a) The problem above stated is a common problem, as for example shown by D3 in point "1. Introduction". Moreover D3 also points out that this problem is well known when using X.509 certificates for authentication (point 2.2 Related Work).
b) The person skilled in the art facing the above stated problem will implement one of the several Proof of Knowledge well known solutions, as for example the "Fiat-Shamir identification protocol" as shown by D2, arriving to the solution proposed by claim 1.
c) Namely the document D2 discloses the missing features of claim 1:
- The certificate comprises publicly available solution information P and a concealed secret S' is publicly available (Pag. 408 l.38).
- The user device providing the verifier device that it knows the secret S without the verifier device learning the secret S or the user identity (Pag. 409 l.1-10).

- Generating a secret S and a solution information P, concealing the secret S into a secret S' (Pag. 408 l.37-38).

d) It is also noted that the certificate re-issuing process is just a mere combination of the anticipated authentication process by D3 and the issuing process of D1, hence not adding any additional distinguishing feature.

3 The same objection above raised to independent claim 1 is also applicable to independent claims 14, 15, 16, 17 and 18. These claims define the corresponding apparatus and software claims to method claim 1.